# Asymptotic Goodness of Expander Codes with Weak Constituent Codes

#### Vitaly Skachek

This work is a part of the speaker's Ph.D. Thesis. It was done at the Technion – Israel Institute of Technology under the supervision of Ron M. Roth.

Vitaly Skachek Asymptotic Goodness of Expander Codes

(日) (四) (日) (日) (日)

Background Basic Definitions LDPC and Low-Complexity Codes Expander Graphs

## LDPC Codes

Low-density parity-check codes.

▶ [Gallager '62] Presented for the first time. Seemed to be unpractical then.

Background Basic Definitions LDPC and Low-Complexity Codes Expander Graphs

## LDPC Codes

Low-density parity-check codes.

- ▶ [Gallager '62] Presented for the first time. Seemed to be unpractical then.
- ▶ [Berrou, Glavieux, Thitimajshima '93] Turbo codes, which are extremely efficient in practice, stimulated a new wave of research on LDPC codes.

(日) (종) (종) (종) (종)

Background Basic Definitions LDPC and Low-Complexity Codes Expander Graphs

## LDPC Codes

Low-density parity-check codes.

- ▶ [Gallager '62] Presented for the first time. Seemed to be unpractical then.
- ▶ [Berrou, Glavieux, Thitimajshima '93] Turbo codes, which are extremely efficient in practice, stimulated a new wave of research on LDPC codes.
- ▶ [Richardson Urbanke '01] Good *average* behavior over binary memoryless channels.

Background Basic Definitions LDPC and Low-Complexity Codes Expander Graphs

## LDPC Codes

Low-density parity-check codes.

- ▶ [Gallager '62] Presented for the first time. Seemed to be unpractical then.
- ▶ [Berrou, Glavieux, Thitimajshima '93] Turbo codes, which are extremely efficient in practice, stimulated a new wave of research on LDPC codes.
- ▶ [Richardson Urbanke '01] Good *average* behavior over binary memoryless channels.
- ▶ [Richardson Shokrollahi Urbanke '01] Codes, which are extremely close to the capacity, found by the exhaustive search.

Background Basic Definitions LDPC and Low-Complexity Codes Expander Graphs

### Explicit Constructions

▶ [Sipser Spielman '96] Correct constant fraction of errors, linear time encoding and decoding.

Vitaly Skachek Asymptotic Goodness of Expander Codes

Background Basic Definitions LDPC and Low-Complexity Codes Expander Graphs

### Explicit Constructions

- ▶ [Sipser Spielman '96] Correct constant fraction of errors, linear time encoding and decoding.
- ▶ [Barg Zémor '01-'04] Capacity-achieving codes for BSC with linear-time decoding, exponentially small decoding error. Binary codes that surpass the Zyablov bound.

(日) (四) (日) (日) (日)

Background Basic Definitions LDPC and Low-Complexity Codes Expander Graphs

### **Basic Definitions**

Vitaly Skachek Asymptotic Goodness of Expander Codes

Background Basic Definitions LDPC and Low-Complexity Codes Expander Graphs

#### **Basic Definitions**

Definition

Code  $\mathcal{C}$  is a set of words of length n over an alphabet  $\Sigma$ .

Vitaly Skachek Asymptotic Goodness of Expander Codes

Background Basic Definitions LDPC and Low-Complexity Codes Expander Graphs

### **Basic** Definitions

#### Definition

Code  $\mathcal{C}$  is a set of words of length n over an alphabet  $\Sigma$ .

### Definition

• The Hamming distance between  $\boldsymbol{x} = (x_1, \ldots, x_n)$  and  $\boldsymbol{y} = (y_1, \ldots, y_n)$  in  $\Sigma^n$ ,  $\mathsf{d}(\boldsymbol{x}, \boldsymbol{y})$ , is the number of pairs of symbols  $(x_i, y_i), 1 \leq i \leq n$ , such that  $x_i \neq y_i$ .

(日) (四) (日) (日) (日)

Background Basic Definitions LDPC and Low-Complexity Codes Expander Graphs

### **Basic Definitions**

#### Definition

Code  $\mathcal{C}$  is a set of words of length n over an alphabet  $\Sigma$ .

### Definition

- ► The Hamming distance between  $\boldsymbol{x} = (x_1, \ldots, x_n)$  and  $\boldsymbol{y} = (y_1, \ldots, y_n)$  in  $\Sigma^n$ ,  $\mathsf{d}(\boldsymbol{x}, \boldsymbol{y})$ , is the number of pairs of symbols  $(x_i, y_i), 1 \leq i \leq n$ , such that  $x_i \neq y_i$ .
- The minimum distance of a code C is

$$d = \min_{\boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}, \boldsymbol{x} \neq \boldsymbol{y}} \mathsf{d}(\boldsymbol{x}, \boldsymbol{y}).$$

(日) (四) (日) (日) (日)

Background Basic Definitions LDPC and Low-Complexity Codes Expander Graphs

### **Basic** Definitions

#### Definition

Code  $\mathcal{C}$  is a set of words of length n over an alphabet  $\Sigma$ .

### Definition

- ► The Hamming distance between  $\boldsymbol{x} = (x_1, \ldots, x_n)$  and  $\boldsymbol{y} = (y_1, \ldots, y_n)$  in  $\Sigma^n$ ,  $\mathsf{d}(\boldsymbol{x}, \boldsymbol{y})$ , is the number of pairs of symbols  $(x_i, y_i), 1 \leq i \leq n$ , such that  $x_i \neq y_i$ .
- The minimum distance of a code C is

$$d = \min_{\boldsymbol{x}, \boldsymbol{y} \in \mathcal{C}, \boldsymbol{x} \neq \boldsymbol{y}} \mathsf{d}(\boldsymbol{x}, \boldsymbol{y}).$$

• The relative minimum distance of C is defined as  $\delta = d/n$ .

(日) (四) (日) (日) (日)

Background Basic Definitions LDPC and Low-Complexity Codes Expander Graphs

## Linear Code

#### Definition

• A code C over field  $\Phi$  is said to be a *linear* [n, k, d] code if there exists a matrix H with n columns and rank n - k such that

$$H \boldsymbol{x}^t = \bar{\boldsymbol{0}} \iff \boldsymbol{x} \in \mathcal{C}.$$

- ▶ The matrix *H* is called a *parity-check matrix*.
- The value k is called the *dimension* of the code C.
- The ratio r = k/n is called the *rate* of the code C.
- ▶ The words of C can be obtained as linear combinations of rows of a generating  $k \times n$  matrix G.

Background Basic Definitions LDPC and Low-Complexity Codes Expander Graphs

# LDPC and Low-Complexity Codes

[Gallager '62]

 Matrix H: the number of non-zero entries in each column (row) of H is typically bounded by a small constant.

Background Basic Definitions LDPC and Low-Complexity Codes Expander Graphs

# LDPC and Low-Complexity Codes

#### [Gallager '62]

- Matrix H: the number of non-zero entries in each column (row) of H is typically bounded by a small constant.
  [Tanner '81]
  - ► A  $\Delta$ -regular undirected graph  $\mathcal{G} = (V, E)$  with |E| = N.

# LDPC and Low-Complexity Codes

#### [Gallager '62]

- Matrix H: the number of non-zero entries in each column (row) of H is typically bounded by a small constant.
  [Tanner '81]
  - ► A  $\Delta$ -regular undirected graph  $\mathcal{G} = (V, E)$  with |E| = N.
  - ► Linear  $[\Delta, k=r\Delta, d=\delta\Delta]$  code C over GF(q).

 $\mathbb{C} = (\mathcal{G}, \mathcal{C})$  is the following linear [N, K, D] code over  $\mathrm{GF}(q) {:}$ 

$$\mathbb{C} = \left\{ \boldsymbol{c} \in (\mathrm{GF}(q))^N : (\boldsymbol{c})_{E(v)} \in \mathcal{C} \text{ for every } v \in V \right\} \ ,$$

 $(c)_{E(v)}$  = the sub-word of c that is indexed by the set of edges incident with v.

# LDPC and Low-Complexity Codes

#### [Gallager '62]

- Matrix H: the number of non-zero entries in each column (row) of H is typically bounded by a small constant.
  [Tanner '81]
  - ► A  $\Delta$ -regular undirected graph  $\mathcal{G} = (V, E)$  with |E| = N.
  - ► Linear  $[\Delta, k=r\Delta, d=\delta\Delta]$  code C over GF(q).

 $\mathbb{C} = (\mathcal{G}, \mathcal{C})$  is the following linear [N, K, D] code over  $\mathrm{GF}(q) {:}$ 

$$\mathbb{C} = \left\{ \boldsymbol{c} \in (\mathrm{GF}(q))^N : (\boldsymbol{c})_{E(v)} \in \mathcal{C} \text{ for every } v \in V \right\} \ ,$$

 $(c)_{E(v)}$  = the sub-word of c that is indexed by the set of edges incident with v.

• The code  $\mathbb{C} = (\mathcal{G}, \mathcal{C})$  is a *low-complexity* code.

Background Basic Definitions LDPC and Low-Complexity Codes Expander Graphs

Low-Complexity Codes – Example

Take  $\Delta = 3$ , k = 2, |V| = 4. Let G be a generating matrix of C over  $F = GF(2^2) = \{0, 1, \alpha, \alpha^2\}$ :

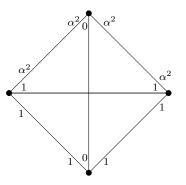
$$G = \left(\begin{array}{rrr} 1 & 0 & 1 \\ 0 & 1 & \alpha \end{array}\right)$$

Background Basic Definitions LDPC and Low-Complexity Codes Expander Graphs

### Low-Complexity Codes – Example

Take  $\Delta = 3$ , k = 2, |V| = 4. Let G be a generating matrix of C over  $F = GF(2^2) = \{0, 1, \alpha, \alpha^2\}$ :

$$G = \left(\begin{array}{rrr} 1 & 0 & 1 \\ 0 & 1 & \alpha \end{array}\right)$$



Background Basic Definitions LDPC and Low-Complexity Codes Expander Graphs

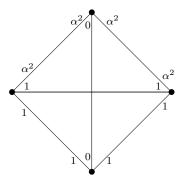
### Low-Complexity Codes – Example

Take 
$$\Delta = 3$$
,  $k = 2$ ,  $|V| = 4$ .  
Let G be a generating matrix of C  
over  $F = GF(2^2) = \{0, 1, \alpha, \alpha^2\}$ :

$$G = \left(\begin{array}{rrr} 1 & 0 & 1 \\ 0 & 1 & \alpha \end{array}\right)$$

The resulting code  $\mathbb{C}$  is of length N = 6. For instance,

$$(1\ 1\ \alpha^2\ 0\ \alpha^2\ 1) \in \mathbb{C}.$$



《曰》 《圖》 《圖》 《圖》

э

Background Basic Definitions LDPC and Low-Complexity Codes Expander Graphs

### Expander Graph

• Consider a  $\Delta$ -regular graph  $\mathcal{G} = (V, E)$ .

Vitaly Skachek Asymptotic Goodness of Expander Codes

Background Basic Definitions LDPC and Low-Complexity Codes Expander Graphs

## Expander Graph

- Consider a  $\Delta$ -regular graph  $\mathcal{G} = (V, E)$ .
- ▶ A subset  $S \subseteq V$  expands by a factor of  $\zeta$ ,  $0 < \zeta \leq 1$ , if

 $|\{v \in V : \exists \tilde{v} \in S \text{ such that } \{v, \tilde{v}\} \in E\}| \ge \zeta \Delta \cdot |S|.$ 

Vitaly Skachek Asymptotic Goodness of Expander Codes

Background Basic Definitions LDPC and Low-Complexity Codes Expander Graphs

## Expander Graph

- Consider a  $\Delta$ -regular graph  $\mathcal{G} = (V, E)$ .
- A subset  $S \subseteq V$  expands by a factor of  $\zeta$ ,  $0 < \zeta \leq 1$ , if

 $|\{v \in V : \exists \tilde{v} \in S \text{ such that } \{v, \tilde{v}\} \in E\}| \ge \zeta \Delta \cdot |S|.$ 

► The graph G is an (α, ζ)-expander if every subset of at most α|V| vertices expands by a factor of ζ.

《曰》 《圖》 《臣》 《臣》 三百

Background Basic Definitions LDPC and Low-Complexity Codes Expander Graphs

## Eigenvalues of Expander Graph

► Consider a graph  $\mathcal{G}$  where each vertex has degree  $\Delta$ . The largest eigenvalue of the adjacency matrix  $A_{\mathcal{G}}$  of  $\mathcal{G}$  is  $\Delta$ .

Background Basic Definitions LDPC and Low-Complexity Codes Expander Graphs

## Eigenvalues of Expander Graph

- ► Consider a graph  $\mathcal{G}$  where each vertex has degree  $\Delta$ . The largest eigenvalue of the adjacency matrix  $A_{\mathcal{G}}$  of  $\mathcal{G}$  is  $\Delta$ .
- Let  $\lambda_{\mathcal{G}}$  be the second largest eigenvalue of  $A_{\mathcal{G}}$ .

Background Basic Definitions LDPC and Low-Complexity Codes Expander Graphs

## Eigenvalues of Expander Graph

- ► Consider a graph  $\mathcal{G}$  where each vertex has degree  $\Delta$ . The largest eigenvalue of the adjacency matrix  $A_{\mathcal{G}}$  of  $\mathcal{G}$  is  $\Delta$ .
- Let  $\lambda_{\mathcal{G}}$  be the second largest eigenvalue of  $A_{\mathcal{G}}$ .
- ► Lower ratios of  $\gamma_{\mathcal{G}} = \frac{\lambda_{\mathcal{G}}}{\Delta}$  correspond to greater values  $\zeta$  of expansion. [Alon '86]

Background Basic Definitions LDPC and Low-Complexity Codes Expander Graphs

Eigenvalues of Expander Graph (cont.)

• Expander graph with

$$\lambda_{\mathcal{G}} \le 2\sqrt{\Delta - 1}$$

is called a Ramanujan graph.

(日) (部) (E) (E) (E)

Background Basic Definitions LDPC and Low-Complexity Codes Expander Graphs

Eigenvalues of Expander Graph (cont.)

• Expander graph with

$$\lambda_{\mathcal{G}} \le 2\sqrt{\Delta - 1}$$

is called a Ramanujan graph.

 Constructions are due to [Lubotsky Philips Sarnak '88], [Margulis '88].

Background Basic Definitions LDPC and Low-Complexity Codes Expander Graphs

Eigenvalues of Expander Graph (cont.)

• Expander graph with

$$\lambda_{\mathcal{G}} \le 2\sqrt{\Delta - 1}$$

is called a Ramanujan graph.

- Constructions are due to [Lubotsky Philips Sarnak '88], [Margulis '88].
- ► For Ramanujan graphs,  $\zeta \approx \frac{1}{2}$ . Eigenvalue approach cannot provide better bounds on  $\zeta$  [Kahale '95].

Background Basic Definitions LDPC and Low-Complexity Codes Expander Graphs

## Expansion of Expander Graph

• Expander graph with  $\zeta = 1 - \epsilon$  is called a *lossless expander*.

Vitaly Skachek Asymptotic Goodness of Expander Codes

Background Basic Definitions LDPC and Low-Complexity Codes Expander Graphs

## Expansion of Expander Graph

- Expander graph with  $\zeta = 1 \epsilon$  is called a *lossless expander*.
- Constructions of *left-regular* bipartite expanders are due to [Reingold Vadhan Wigderson '00], [Capalbo *et al.* '02].

Background Basic Definitions LDPC and Low-Complexity Codes Expander Graphs

## Expansion of Expander Graph

- Expander graph with  $\zeta = 1 \epsilon$  is called a *lossless expander*.
- Constructions of *left-regular* bipartite expanders are due to [Reingold Vadhan Wigderson '00], [Capalbo *et al.* '02].

• For these graphs, 
$$\gamma_{\mathcal{G}} = O(1/\Delta^{1/3})$$
.

Construction Example Parameters

## Expander Code Construction

[Sipser Spielman '96], [Barg Zémor '01 - '04].

• Graph  $\mathcal{G} = (V, E)$  is a  $\Delta$ -regular bipartite undirected graph.

Construction Example Parameters

### Expander Code Construction

[Sipser Spielman '96], [Barg Zémor '01 - '04].

- ► Graph  $\mathcal{G} = (V, E)$  is a  $\Delta$ -regular bipartite undirected graph.
  - ▶ Vertex set  $V = A \cup B$  such that  $A \cap B = \emptyset$  and |A| = |B| = n.
  - Edge set E of size  $n\Delta$  such that every edge in E has one endpoint in A and one endpoint in B.

Construction Example Parameters

### Expander Code Construction

[Sipser Spielman '96], [Barg Zémor '01 - '04].

- ► Graph  $\mathcal{G} = (V, E)$  is a  $\Delta$ -regular bipartite undirected graph.
  - ▶ Vertex set  $V = A \cup B$  such that  $A \cap B = \emptyset$  and |A| = |B| = n.
  - Edge set E of size  $n\Delta$  such that every edge in E has one endpoint in A and one endpoint in B.
- ► Linear  $[\Delta, k=r_A\Delta, \delta_A\Delta]$  and  $[\Delta, r_B\Delta, \delta_B\Delta]$  codes  $C_A$  and  $C_B$ , respectively, over F = GF(q).

Construction Example Parameters

Expander Code Construction (cont.)

 $\mathbb{C}$  is a linear code of length |E| over F:

$$\mathbb{C} = \left\{ \boldsymbol{c} \in F^{|E|} : \begin{array}{c} (\boldsymbol{c})_{E(u)} \in \mathcal{C}_A \text{ for every } u \in A \text{ and} \\ (\boldsymbol{c})_{E(u)} \in \mathcal{C}_B \text{ for every } u \in B \end{array} \right\} ,$$

where  $(c)_{E(u)}$  = the sub-word of c that is indexed by the set of edges incident with u.

Construction Example Parameters

# Example

Take k = 2,  $\Delta = 3$ , n = 4. Let  $G_A$  and  $G_B$  be generating matrices of  $\mathcal{C}_A$  and  $\mathcal{C}_B$ (respectively) over  $F = \operatorname{GF}(2^2) = \{0, 1, \alpha, \alpha^2\}$ :

$$G_A = \left(\begin{array}{rrr} 1 & 1 & 1 \\ 1 & \alpha & 0 \end{array}\right) \ ,$$
$$G_B = \left(\begin{array}{rrr} 1 & 0 & 1 \\ 0 & 1 & \alpha \end{array}\right) \ .$$

Vitaly Skachek

Asymptotic Goodness of Expander Codes

(日) (四) (日) (日) (日)

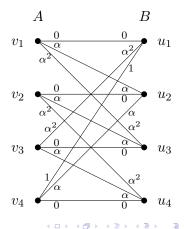
Construction Example Parameters

# Example

Take 
$$k = 2$$
,  $\Delta = 3$ ,  $n = 4$ .  
Let  $G_A$  and  $G_B$  be generating  
matrices of  $\mathcal{C}_A$  and  $\mathcal{C}_B$   
(respectively) over  
 $F = \operatorname{GF}(2^2) = \{0, 1, \alpha, \alpha^2\}$ :

$$G_A = \left(\begin{array}{rrr} 1 & 1 & 1 \\ 1 & \alpha & 0 \end{array}\right) \;,$$
$$G_B = \left(\begin{array}{rrr} 1 & 0 & 1 \\ 0 & 1 & \alpha \end{array}\right) \;.$$

Vitaly Skachek



Asymptotic Goodness of Expander Codes

Construction Example Parameters

## Parameters of Expander Codes

The Code Rate

 $\mathcal{R} \ge r_A + r_B - 1.$ 

Vitaly Skachek Asymptotic Goodness of Expander Codes

Construction Example Parameters

Parameters of Expander Codes

#### The Code Rate

$$\mathcal{R} \ge r_A + r_B - 1.$$

Relative Minimum Distance [Roth Skachek '04]

$$D \ge N \cdot \frac{\delta_A \delta_B - \gamma_{\mathcal{G}} \sqrt{\delta_A \delta_B}}{1 - \gamma_{\mathcal{G}}} \, .$$

(日) (종) (종) (종) (종)

**Definition and Known Results** Codes of Minimum Distance 2 Tree-Based Lower Bound Sufficient Condition

# Asymptotic Goodness

#### Definition

A family of codes  $\{C_i\}_{i=0}^{\infty}$ , where each  $C_i$  is a  $[n_i, k_i, d_i]$  linear code, is said to be *asymptotically good* if it satisfies the following conditions:

▶ The length  $n_i$  of  $C_i$  approaches infinity as  $i \to \infty$ .

**Definition and Known Results** Codes of Minimum Distance 2 Tree-Based Lower Bound Sufficient Condition

# Asymptotic Goodness

#### Definition

A family of codes  $\{C_i\}_{i=0}^{\infty}$ , where each  $C_i$  is a  $[n_i, k_i, d_i]$  linear code, is said to be *asymptotically good* if it satisfies the following conditions:

▶ The length  $n_i$  of  $C_i$  approaches infinity as  $i \to \infty$ .

$$\blacktriangleright \lim_{i \to \infty} \frac{d_i}{n_i} = \delta > 0$$

**Definition and Known Results** Codes of Minimum Distance 2 Tree-Based Lower Bound Sufficient Condition

# Asymptotic Goodness

#### Definition

A family of codes  $\{C_i\}_{i=0}^{\infty}$ , where each  $C_i$  is a  $[n_i, k_i, d_i]$  linear code, is said to be *asymptotically good* if it satisfies the following conditions:

▶ The length  $n_i$  of  $C_i$  approaches infinity as  $i \to \infty$ .

$$\blacktriangleright \lim_{i \to \infty} \frac{d_i}{n_i} = \delta > 0$$

$$\blacktriangleright \lim_{i\to\infty} \frac{k_i}{n_i} = \mathcal{R} > 0$$

Definition and Known Results Codes of Minimum Distance 2 Tree-Based Lower Bound Sufficient Condition

# Asymptotic Goodness

#### Definition

A family of codes  $\{C_i\}_{i=0}^{\infty}$ , where each  $C_i$  is a  $[n_i, k_i, d_i]$  linear code, is said to be *asymptotically good* if it satisfies the following conditions:

• The length  $n_i$  of  $C_i$  approaches infinity as  $i \to \infty$ .

$$\blacktriangleright \lim_{i \to \infty} \frac{d_i}{n_i} = \delta > 0$$

$$\blacktriangleright \lim_{i\to\infty} \frac{k_i}{n_i} = \mathcal{R} > 0$$

#### **Problem Statement**

How weak the constituent codes  $C_A$  and  $C_B$  could be such that the overall expander code will be asymptotically good?

(日) (四) (日) (日) (日)

**Definition and Known Results** Codes of Minimum Distance 2 Tree-Based Lower Bound Sufficient Condition

### Asymptotic Goodness – Some Answers

The bound on the minimum distance:

$$\delta \geq \frac{\delta_A \delta_B - \gamma_{\mathcal{G}} \sqrt{\delta_A \delta_B}}{1 - \gamma_{\mathcal{G}}}$$

Vitaly Skachek Asymptotic Goodness of Expander Codes

**Definition and Known Results** Codes of Minimum Distance 2 Tree-Based Lower Bound Sufficient Condition

### Asymptotic Goodness – Some Answers

The bound on the minimum distance:

$$\delta \geq \frac{\delta_A \delta_B - \gamma_{\mathcal{G}} \sqrt{\delta_A \delta_B}}{1 - \gamma_{\mathcal{G}}}$$

yields the sufficient condition

$$\sqrt{d_A d_B} > \gamma_{\mathcal{G}} \Delta = \lambda_{\mathcal{G}}$$

**Definition and Known Results** Codes of Minimum Distance 2 Tree-Based Lower Bound Sufficient Condition

### Asymptotic Goodness – Some Answers

The bound on the minimum distance:

$$\delta \geq \frac{\delta_A \delta_B - \gamma_{\mathcal{G}} \sqrt{\delta_A \delta_B}}{1 - \gamma_{\mathcal{G}}}$$

yields the sufficient condition

$$\sqrt{d_A d_B} > \gamma_{\mathcal{G}} \Delta = \lambda_{\mathcal{G}} \ge 2\sqrt{\Delta - 1}$$
.

**Definition and Known Results** Codes of Minimum Distance 2 Tree-Based Lower Bound Sufficient Condition

Asymptotic Goodness – Some Answers (cont.)

[Sipser Spielman '96]

• Codes  $C_A$  with  $d_A = \Delta$  and  $C_B$  with  $d_B = 2$ .

Vitaly Skachek Asymptotic Goodness of Expander Codes

**Definition and Known Results** Codes of Minimum Distance 2 Tree-Based Lower Bound Sufficient Condition

Asymptotic Goodness – Some Answers (cont.)

[Sipser Spielman '96]

- Codes  $C_A$  with  $d_A = \Delta$  and  $C_B$  with  $d_B = 2$ .
- Bipartite  $(\alpha, \zeta)$ -expander graph with  $\zeta \geq 3/4$ .

(日) (四) (日) (日) (日)

**Definition and Known Results** Codes of Minimum Distance 2 Tree-Based Lower Bound Sufficient Condition

Asymptotic Goodness – Some Answers (cont.)

[Sipser Spielman '96]

- Codes  $C_A$  with  $d_A = \Delta$  and  $C_B$  with  $d_B = 2$ .
- Bipartite  $(\alpha, \zeta)$ -expander graph with  $\zeta \geq 3/4$ .
- $\blacktriangleright \qquad \Rightarrow \qquad \text{Relative minimum distance is at least } \alpha.$

Definition and Known Results Codes of Minimum Distance 2 Tree-Based Lower Bound Sufficient Condition

Asymptotic Goodness – Some Answers (cont.)

#### [Sipser Spielman '96]

- Codes  $C_A$  with  $d_A = \Delta$  and  $C_B$  with  $d_B = 2$ .
- Bipartite  $(\alpha, \zeta)$ -expander graph with  $\zeta \geq 3/4$ .
- $\blacktriangleright \qquad \Rightarrow \qquad \text{Relative minimum distance is at least } \alpha.$

#### [Barg Zémor '04]

• Codes  $C_A$  with  $d_A \ge 3$  and  $C_B$  with  $d_B \ge 3$ .

(日) (四) (日) (日) (日)

Definition and Known Results Codes of Minimum Distance 2 Tree-Based Lower Bound Sufficient Condition

Asymptotic Goodness – Some Answers (cont.)

#### [Sipser Spielman '96]

- Codes  $C_A$  with  $d_A = \Delta$  and  $C_B$  with  $d_B = 2$ .
- Bipartite  $(\alpha, \zeta)$ -expander graph with  $\zeta \geq 3/4$ .
- $\Rightarrow \qquad \text{Relative minimum distance is at least } \alpha.$

#### [Barg Zémor '04]

- Codes  $C_A$  with  $d_A \ge 3$  and  $C_B$  with  $d_B \ge 3$ .
- ▶ Random bipartite graph.

(日) (四) (日) (日) (日)

Definition and Known Results Codes of Minimum Distance 2 Tree-Based Lower Bound Sufficient Condition

Asymptotic Goodness – Some Answers (cont.)

#### [Sipser Spielman '96]

- Codes  $C_A$  with  $d_A = \Delta$  and  $C_B$  with  $d_B = 2$ .
- Bipartite  $(\alpha, \zeta)$ -expander graph with  $\zeta \geq 3/4$ .
- $\Rightarrow \qquad \text{Relative minimum distance is at least } \alpha.$

#### [Barg Zémor '04]

- Codes  $C_A$  with  $d_A \ge 3$  and  $C_B$  with  $d_B \ge 3$ .
- ▶ Random bipartite graph.
- $\blacktriangleright \Rightarrow \qquad \text{Relative minimum distance is bounded away} \\ \text{from zero with probability close to 1.} \\$

Definition and Known Results Codes of Minimum Distance 2 Tree-Based Lower Bound Sufficient Condition

## Constituent Codes of Minimum Distance 2

#### Example

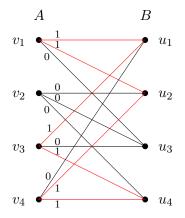
Take k = 2,  $\Delta = 3$ , n = 4. Let  $C_A$  and  $C_B$  be binary parity codes.

Definition and Known Results Codes of Minimum Distance 2 Tree-Based Lower Bound Sufficient Condition

## Constituent Codes of Minimum Distance 2

#### Example

Take k = 2,  $\Delta = 3$ , n = 4. Let  $C_A$  and  $C_B$  be binary parity codes.



<ロト <問ト < 国ト < 国ト

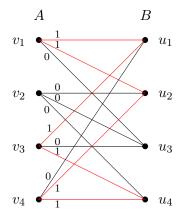
Definition and Known Results Codes of Minimum Distance 2 Tree-Based Lower Bound Sufficient Condition

# Constituent Codes of Minimum Distance 2

#### Example

Take k = 2,  $\Delta = 3$ , n = 4. Let  $C_A$  and  $C_B$  be binary parity codes.

• Every non-zero pattern contains a cycle.



<ロト <問ト < 国ト < 国ト

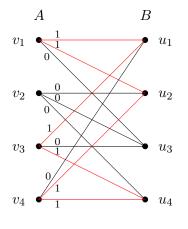
Definition and Known Results Codes of Minimum Distance 2 Tree-Based Lower Bound Sufficient Condition

# Constituent Codes of Minimum Distance 2

#### Example

Take k = 2,  $\Delta = 3$ , n = 4. Let  $C_A$  and  $C_B$  be binary parity codes.

- Every non-zero pattern contains a cycle.
- Every cycle can be converted into a legal non-zero pattern.



< ロト < 同ト < ヨト < ヨト

Constituent Codes of Minimum Distance 2 (cont.)

#### Theorem

Let  $C_A$  and  $C_B$  be codes of minimum distance 2, and let  $\mathcal{G}$  be any  $\Delta$ -regular bipartite graph. Then, the minimum distance of such code  $\mathbb{C}$  is bounded from above by

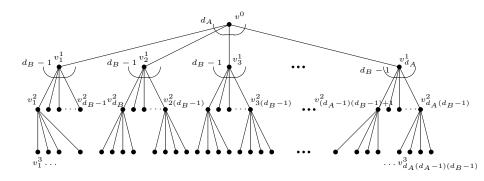
$$D \le O\left(\log_{\Delta - 1}(n)\right)$$
.

Moreover, if the underlying graph  $\mathcal{G}$  is a Ramanujan graph as in [Lubotsky Philips Sarnak '88] or [Margulis '88], then the minimum distance of  $\mathbb{C}$  is bounded from below by

$$D \ge \frac{4}{3} \log_{\Delta - 1}(2n) \; .$$

Definition and Known Results Codes of Minimum Distance 2 **Tree-Based Lower Bound** Sufficient Condition

### Tree-Based Lower Bound



Vitaly Skachek Asymptotic Goodness of Expander Codes

<ロト <問ト < 国ト < 国ト

# Tree-Based Lower Bound (cont.)

#### Theorem

Consider the code  $\mathbb{C}$  with the constituent codes  $C_A$  and  $C_B$  of minimum distance  $d_A \geq 2$  and  $d_B \geq 2$ , respectively, with the underlying graph  $\mathcal{G}$  as in [Lubotsky Philips Sarnak '88] or [Margulis '88]. Then, its relative minimum distance is bounded from below by

$$D \ge (2n)^{1/3 \cdot \log_{\Delta - 1}(d_A - 1)(d_B - 1)} - 1$$
.

(日) (四) (日) (日) (日)

Definition and Known Results Codes of Minimum Distance 2 Tree-Based Lower Bound Sufficient Condition

## Sufficient Condition

#### Theorem

Let  $C_A$  and  $C_B(u)$  (for every  $u \in B$ ) be linear codes with the minimum distance  $d_A = \delta_A \Delta$  and  $d_B$ , respectively. Let  $\mathcal{G}$  be a bipartite  $(\alpha, \zeta)$ -expander such that the degree of every  $u \in A$ is  $\Delta$ . If

$$\frac{\delta_A}{\zeta + \delta_A - 1} < d_B \; ,$$

then the relative minimum distance of  $\mathbb{C}$  is  $\geq \alpha \delta_A$ .

Definition and Known Results Codes of Minimum Distance 2 Tree-Based Lower Bound Sufficient Condition

## Improvement over the Known Results

Example

• Ramanujan graph with  $\zeta \approx \frac{1}{2}$ .

(日) (종) (종) (종) (종)

Definition and Known Results Codes of Minimum Distance 2 Tree-Based Lower Bound Sufficient Condition

# Improvement over the Known Results

## Example

- Ramanujan graph with  $\zeta \approx \frac{1}{2}$ .
- Code  $C_A$  with  $\delta_A = 1$  and code  $C_B(u)$  with  $d_B = 3$ .

(日) (四) (日) (日) (日)

## Improvement over the Known Results

### Example

- Ramanujan graph with  $\zeta \approx \frac{1}{2}$ .
- Code  $C_A$  with  $\delta_A = 1$  and code  $C_B(u)$  with  $d_B = 3$ .
- ► Then,

$$\frac{\delta_A}{\zeta + \delta_A - 1} < d_B \; .$$

《曰》 《聞》 《臣》 《臣》

# Improvement over the Known Results

### Example

- Ramanujan graph with  $\zeta \approx \frac{1}{2}$ .
- Code  $C_A$  with  $\delta_A = 1$  and code  $C_B(u)$  with  $d_B = 3$ .

► Then,

$$\frac{\delta_A}{\zeta + \delta_A - 1} < d_B \; .$$

 $\blacktriangleright \qquad \Rightarrow \qquad \text{Relative minimum distance of } \mathbb{C} \text{ is } \geq \alpha \delta_A.$ 

(日) (四) (日) (日) (日)

# Improvement over the Known Results

## Example

- Ramanujan graph with  $\zeta \approx \frac{1}{2}$ .
- Code  $C_A$  with  $\delta_A = 1$  and code  $C_B(u)$  with  $d_B = 3$ .

► Then,

$$\frac{\delta_A}{\zeta + \delta_A - 1} < d_B \; .$$

⇒ Relative minimum distance of C is ≥ αδ<sub>A</sub>.
The previously-known bound does not lead to any interesting result.

(日) (四) (日) (日) (日)

Conclusions

### Further Research

 We showed necessary and sufficient condition for asymptotic goodness of expander codes.

## Further Research

- ▶ We showed necessary and sufficient condition for asymptotic goodness of expander codes.
- ▶ We presented new bounds on the minimum distance of expander codes.

# Further Research

- ▶ We showed necessary and sufficient condition for asymptotic goodness of expander codes.
- ▶ We presented new bounds on the minimum distance of expander codes.
- ▶ The new condition improves on the known results for a range of parameters.

(日) (종) (종) (종) (종)

# Further Research

- ▶ We showed necessary and sufficient condition for asymptotic goodness of expander codes.
- ▶ We presented new bounds on the minimum distance of expander codes.
- ▶ The new condition improves on the known results for a range of parameters.
- ▶ Tight (necessary and sufficient) conditions are still remain an open problem...